

Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty



NEW QUESTION 1

A company deployed IAM Organizations to help manage its increasing number of IAM accounts. A security engineer wants to ensure only principals in the Organization structure can access a specific Amazon S3 bucket. The solution must also minimize operational overhead. Which solution will meet these requirements?

- A. Put all users into an IAM group with an access policy granting access to the bucket.
- B. Have the account creation trigger an IAM Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
- C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
- D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

NEW QUESTION 2

A company wants to protect its website from man-in-the-middle attacks by using Amazon CloudFront. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use the SimpleCORS managed response headers policy.
- B. Use a Lambda@Edge function to add the Strict-Transport-Security response header.
- C. Use the SecurityHeadersPolicy managed response headers policy.
- D. Include the X-XSS-Protection header in a custom response headers policy.

Answer: C

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-managed-response-headers-policy.html> The SecurityHeadersPolicy is a managed policy provided by Amazon CloudFront that includes a set of recommended security headers to enhance the security of your website. These headers help protect against various types of attacks, including man-in-the-middle attacks. By applying the SecurityHeadersPolicy to your CloudFront distribution, the necessary security headers will be automatically added to the responses sent by CloudFront. This reduces operational overhead because you don't have to manually configure or manage the headers yourself.

NEW QUESTION 3

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.

Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role.
- B. Configure the state machine to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role.
- D. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- F. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- G. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- H. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.
- I. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices.
- J. Subscribe the security team's email addresses to the topic.

Answer: ACF

Explanation:

The correct answer is A, C, and F.

To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents.

Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses.

Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response.

Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings.

Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job.

Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for messages. However, SQS cannot directly forward a notification to the security team's email addresses. You would need to use another service such as SNS or SES to send email notifications.

Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team's email addresses to the topic is a valid way to notify the security incidents. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can use SNS to send email notifications to the security team when a critical security finding is detected.

References:

- > AWS Step Functions
- > AWS Batch
- > Amazon EventBridge
- > Amazon CloudWatch
- > Amazon SQS
- > Amazon SNS

NEW QUESTION 4

A company has retail stores The company is designing a solution to store scanned copies of customer receipts on Amazon S3 Files will be between 100 KB and 5 MB in PDF format Each retail store must have a unique encryption key Each object must be encrypted with a unique key Which solution will meet these requirements?

- A. Create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store Use the S3 Put operation to upload the objects to Amazon S3 Specify server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key
- B. Create a new AWS Key Management Service (AWS KMS) customer managed key every day for each retail store Use the KMS Encrypt operation to encrypt objects Then upload the objects to Amazon S3
- C. Run the AWS Key Management Service (AWS KMS) GenerateDataKey operation every day for each retail store Use the data key and client-side encryption to encrypt the objects Then upload the objects to Amazon S3
- D. Use the AWS Key Management Service (AWS KMS) ImportKeyMaterial operation to import new key material to AWS KMS every day for each retail store Use a customer managed key and the KMS Encrypt operation to encrypt the objects Then upload the objects to Amazon S3

Answer: A

Explanation:

To meet the requirements of storing scanned copies of customer receipts on Amazon S3, where files will be between 100 KB and 5 MB in PDF format, each retail store must have a unique encryption key, and each object must be encrypted with a unique key, the most appropriate solution would be to create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store. Then, use the S3 Put operation to upload the objects to Amazon S3, specifying server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key.

References: : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Services : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Service

NEW QUESTION 5

A company has two IAM accounts within IAM Organizations. In Account-1. Amazon EC2 Auto Scaling is launched using a service-linked role. In Account-2. Amazon EBS volumes are encrypted with an IAM KMS key A Security Engineer needs to ensure that the service-linked role can launch instances with these encrypted volumes

Which combination of steps should the Security Engineer take in both accounts? (Select TWO.)

- A. Allow Account-1 to access the KMS key in Account-2 using a key policy
- B. Attach an IAM policy to the service-linked role in Account-1 that allows these actions CreateGrant, DescnbeKey, Encrypt, GenerateDataKey, Decrypt, and ReEncrypt
- C. Create a KMS grant for the service-linked role with these actions CreateGrant, DescnbeKey Encrypt GenerateDataKey Decrypt, and ReEncrypt
- D. Attach an IAM policy to the role attached to the EC2 instances with KMS actions and then allow Account-1 in the KMS key policy.
- E. Attach an IAM policy to the user who is launching EC2 instances and allow the user to access the KMS key policy of Account-2.

Answer: CD

Explanation:

because these are the steps that can ensure that the service-linked role can launch instances with encrypted volumes. A service-linked role is a type of IAM role that is linked to an AWS service and allows the service to perform actions on your behalf. A KMS grant is a mechanism that allows you to delegate permissions to use a customer master key (CMK) to a principal such as a service-linked role. A KMS grant specifies the actions that the principal can perform, such as encrypting and decrypting data. By creating a KMS grant for the service-linked role with the specified actions, you can allow the service-linked role to use the CMK in Account-2 to launch instances with encrypted volumes. By attaching an IAM policy to the role attached to the EC2 instances with KMS actions and then allowing Account-1 in the KMS key policy, you can also enable cross-account access to the CMK and allow the EC2 instances to use the encrypted volumes. The other options are either incorrect or unnecessary for meeting the requirement.

NEW QUESTION 6

A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region. The DB cluster is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. To meet compliance requirements, the company needs to copy a DB snapshot to the us-west-1 Region. However, when the company tries to copy the snapshot to us-west-1 the company cannot access the key that was used to encrypt the original database.

What should the company do to set up the snapshot in us-west-1 with proper encryption?

- A. Use AWS Secrets Manager to store the customer managed key in us-west-1 as a secret Use this secret to encrypt the snapshot in us-west-1.
- B. Create a new customer managed key in us-west-1. Use this new key to encrypt the snapshot in us-west-1.
- C. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify am aws kmsus-west-1 " as the principal.
- D. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify arn aws rds us-west-1. * as the principal.

Answer: B

Explanation:

"If you copy an encrypted snapshot across Regions, you must specify a KMS key valid in the destination AWS Region. It can be a Region-specific KMS key, or a multi-Region key." <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-copy-snapshot.html#aurora-copy-sna>

NEW QUESTION 7

A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud. Which solution will meet these requirements?

- A. Do not use SSH-RSA private keys during the launch of new instance
- B. Implement AWS Systems Manager Session Manager.
- C. Generate new SSH-RSA private keys for existing instance
- D. Implement AWS Systems Manager Session Manager.
- E. Do not use SSH-RSA private keys during the launch of new instance
- F. Configure EC2 Instance Connect.
- G. Generate new SSH-RSA private keys for existing instance
- H. Configure EC2 Instance Connect.

Answer: A

Explanation:

AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.

EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.

The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.

Verified References:

- > <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>
- > <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html>
- > <https://repost.aws/questions/QUv4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-ins>

NEW QUESTION 8

A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access. Which actions must the Security Engineer take to address these audit findings? (Select THREE)

- A. Ensure CloudTrail log file validation is turned on
- B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage
- C. Use an S3 bucket with tight access controls that exists in a separate account
- D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.
- E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files
- F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

Answer: ADE

NEW QUESTION 9

An ecommerce website was down for 1 hour following a DDoS attack. Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events. The company needs to minimize downtime in its response to similar attacks in the future.

Which steps would help achieve this? (Select TWO)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
- B. Subscribe to IAM Shield Advanced and reach out to IAM Support in the event of an attack.
- C. Use VPC Flow Logs to monitor network traffic and an IAM Lambda function to automatically block an attacker's IP using security groups.
- D. Set up an Amazon CloudWatch Events rule to monitor the IAM CloudTrail events in real time, use IAM Config rules to audit the configuration, and use IAM Systems Manager for remediation.
- E. Use IAM WAF to create rules to respond to such attacks.

Answer: BE

Explanation:

To minimize downtime in response to DDoS attacks, the company should do the following:

- > Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack. This provides access to 24x7 support from the AWS DDoS Response Team (DRT), as well as advanced detection and mitigation capabilities for network and application layer attacks.
- > Use AWS WAF to create rules to respond to such attacks. This allows the company to filter web requests based on IP addresses, headers, body, or URI strings, and block malicious requests before they reach the web applications.

NEW QUESTION 10

A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1 Region. Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at rest. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.

The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.

After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.

Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

- A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.

- B. Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects.
- C. Encrypt permission for the key in us-east-1 that encrypts source objects.
- D. Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.
- E. Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.
- F. Decrypt permission for the key in us-east-1 that encrypts source objects.
- G. Change the key policy of the key in us-east-1 to grant the kms.Decrypt permission to the security engineer's IAM account.
- H. Decrypt permission to the security engineer's IAM account.
- I. Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

Answer: BF

Explanation:

To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

➤ Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects. This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

➤ Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role.

This solution will remediate the issue of encrypted objects not being replicated to the destination bucket.

The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).

Verified References:

➤ <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>

NEW QUESTION 10

A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:

Developer group permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
  ]
}
```

Production account 999999999999:

Production account ReadS3 role policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ]
    }
  ]
}
```

Production account ReadS3 role policy - trust relationship:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::888888888888:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": "true"
        }
      }
    }
  ]
}
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

- A. Ask the developers to change their password and use a different web browser.
- B. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.
- C. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.
- D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.
- E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

Answer: AD

NEW QUESTION 11

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139).

The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What action should be performed to allow the ping to work?

- A. In the security group of the EC2 instance, allow inbound ICMP traffic.
- B. In the security group of the EC2 instance, allow outbound ICMP traffic.
- C. In the VPC's NACL, allow inbound ICMP traffic.
- D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: D

NEW QUESTION 13

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks. A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly. How should the security engineer build the MOST secure solution?

- A. Add an origin custom header. Set the viewer protocol policy to HTTP and HTTPS. Set the origin protocol policy to HTTPS only. Update the application to validate the CloudFront custom header.
- B. Add an origin custom header. Set the viewer protocol policy to HTTPS only. Set the origin protocol policy to match viewer. Update the application to validate the CloudFront custom header.
- C. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS. Set the origin protocol policy to HTTP only. Update the application to validate the CloudFront custom header.
- D. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS.
- E. Set the origin protocol policy to HTTPS only. Update the application to validate the CloudFront custom header.

Answer: D

Explanation:

To ensure that application content is accessible only through CloudFront and not directly, the security engineer should do the following:

- Add an origin custom header. This is a header that CloudFront adds to the requests that it sends to the origin, but viewers cannot see or modify.
- Set the viewer protocol policy to redirect HTTP to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront.
- Set the origin protocol policy to HTTPS only. This ensures that CloudFront always uses HTTPS when it connects to the origin.
- Update the application to validate the CloudFront custom header. This means that the application checks if the request has the custom header and only responds if it does. Otherwise, it denies or ignores the request. This prevents users from bypassing CloudFront and accessing the content directly on the origin.

NEW QUESTION 15

A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database. During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual. Which combination of options can the company use to meet these requirements? (Select TWO.)

- A. Create a snapshot of the DB instance.
- B. Copy the snapshot to a new snapshot, and enable encryption for the copy process.
- C. Use the new snapshot to restore the DB instance.
- D. Modify the configuration of the DB instance by enabling encryption.
- E. Create a snapshot of the DB instance.
- F. Use the snapshot to restore the DB instance.
- G. Use IAM Key Management Service (IAM KMS) to create a new default IAM managed AWS KMS key. Select this key as the encryption key for operations with Amazon RDS.
- H. Use IAM Key Management Service (IAM KMS) to create a new CMK.
- I. Select this key as the encryption key for operations with Amazon RDS.
- J. Create a snapshot of the DB instance.
- K. Enable encryption on the snapshot. Use the snapshot to restore the DB instance.

Answer: CE

NEW QUESTION 20

A company has a new partnership with a vendor. The vendor will process data from the company's customers. The company will upload data files as objects into an Amazon S3 bucket. The vendor will download the objects to perform data processing. The objects will contain sensitive data. A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours. Which solution will meet these requirements?

- A. Use Amazon Macie to scan the S3 bucket for sensitive data every 72 hours.
- B. Configure Macie to delete the objects that contain sensitive data when they are discovered.
- C. Configure an S3 Lifecycle rule on the S3 bucket to expire objects that have been in the S3 bucket for 72 hours.
- D. Create an Amazon EventBridge scheduled rule that invokes an AWS Lambda function every day. Program the Lambda function to remove any objects that have been in the S3 bucket for 72 hours.
- E. Use the S3 Intelligent-Tiering storage class for all objects that are uploaded to the S3 bucket.
- F. Use S3 Intelligent-Tiering to expire objects that have been in the S3 bucket for 72 hours.

Answer: B

NEW QUESTION 22

A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates. After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume. Which solution will meet these requirements?

- A. Turn on AWS Trusted Advisor.
- B. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.
- C. Turn on AWS Config.
- D. Use the prebuilt rules or customized rule.
- E. Subscribe the CI/CD pipeline to an Amazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.

- F. Create rule sets in AWS CloudFormation Guar
- G. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
- H. Create rule sets as SCP
- I. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.

Answer: C

Explanation:

The correct answer is C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process. This answer is correct because AWS CloudFormation Guard is a tool that helps you implement policy-as-code for your CloudFormation templates. You can use Guard to write rules that define your security policies, such as requiring encryption for EBS volumes, and then validate your templates against those rules before deploying them. You can integrate Guard into your CI/CD pipeline as a step that runs the validation checks and prevents the deployment of any non-compliant templates¹².

The other options are incorrect because:

- > A. Turning on AWS Trusted Advisor and configuring security notifications as webhooks in the preferences section of the CI/CD pipeline is not a solution, because AWS Trusted Advisor is not a policy-as-code tool, but a service that provides recommendations to help you follow AWS best practices. Trusted Advisor does not allow you to define your own security policies or validate your CloudFormation templates against them³.
- > B. Turning on AWS Config and using the prebuilt or customized rules is not a solution, because AWS Config is not a policy-as-code tool, but a service that monitors and records the configuration changes of your AWS resources. AWS Config does not allow you to validate your CloudFormation templates before deploying them, but only evaluates the compliance of your resources after they are created⁴.
- > D. Creating rule sets as SCPs and integrating them as a part of validation control in a phase of the CI/CD process is not a solution, because SCPs are not policy-as-code tools, but policies that you can use to manage permissions in your AWS Organizations. SCPs do not allow you to validate your CloudFormation templates, but only restrict the actions that users and roles can perform in your accounts⁵.

References:

- 1: What is AWS CloudFormation Guard? 2: Introducing AWS CloudFormation Guard 2.0 3: AWS Trusted Advisor 4: What Is AWS Config? 5: Service control policies - AWS Organizations

NEW QUESTION 24

A company has two teams, and each team needs to access its respective Amazon S3 buckets. The company anticipates adding more teams that also will have their own S3 buckets. When the company adds these teams, team members will need the ability to be assigned to multiple teams. Team members also will need the ability to change teams. Additional S3 buckets can be created or deleted.

An IAM administrator must design a solution to accomplish these goals. The solution also must be scalable and must require the least possible operational overhead.

Which solution meets these requirements?

- A. Add users to groups that represent the team
- B. Create a policy for each team that allows the team to access its respective S3 buckets onl
- C. Attach the policy to the corresponding group.
- D. Create an IAM role for each tea
- E. Create a policy for each team that allows the team to access its respective S3 buckets onl
- F. Attach the policy to the corresponding role.
- G. Create IAM roles that are labeled with an access tag value of a tea
- H. Create one policy that allows dynamic access to S3 buckets with the same ta
- I. Attach the policy to the IAM role
- J. Tag the S3 buckets accordingly.
- K. Implement a role-based access control (RBAC) authorization mode
- L. Create the corresponding policies, and attach them to the IAM users.

Answer: A

NEW QUESTION 28

A company is building a data processing application mat uses AWS Lambda functions. The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account

Which solution meets these requirements in the MOST secure way?

- A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
- B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0
- C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
- D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Answer: C

Explanation:

This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

NEW QUESTION 31

A security engineer needs to develop a process to investigate and respond to po-tential security events on a company's Amazon EC2 instances. All the EC2 instances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.

The process that the security engineer is developing must comply with AWS secu-rity best practices and must meet the following requirements:

- A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
- A compromised EC2 instance's metadata must be updated with corresponding inci-dent ticket information.
- A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.

• Any investigative activity during the collection of volatile data must be captured as part of the process. Which combination of steps should the security engineer take to meet these requirements with the LEAST operational overhead? (Select THREE.)

- A. Gather any relevant metadata for the compromised EC2 instance
- B. Enable termination protection
- C. Isolate the instance by updating the instance's security groups to restrict access
- D. Detach the instance from any Auto Scaling groups that the instance is a member of
- E. Deregister the instance from any Elastic Load Balancing (ELB) resources.
- F. Gather any relevant metadata for the compromised EC2 instance
- G. Enable termination protection
- H. Move the instance to an isolation subnet that denies all source and destination traffic
- I. Associate the instance with the subnet to restrict access
- J. Detach the instance from any Auto Scaling groups that the instance is a member of
- K. Deregister the instance from any Elastic Load Balancing (ELB) resources.
- L. Use Systems Manager Run Command to invoke scripts that collect volatile data.
- M. Establish a Linux SSH or Windows Remote Desktop Protocol (RDP) session to the compromised EC2 instance to invoke scripts that collect volatile data.
- N. Create a snapshot of the compromised EC2 instance's EBS volume for follow-up investigation
- O. Tag the instance with any relevant metadata and incident ticket information.
- P. Create a Systems Manager State Manager association to generate an EBS volume snapshot of the compromised EC2 instance
- Q. Tag the instance with any relevant metadata and incident ticket information.

Answer: ACE

NEW QUESTION 34

A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account. Which solution will meet this requirement?

- A. Use Macie to detect an active DDoS event
- B. Create Amazon CloudWatch alarms that respond to Macie findings.
- C. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.
- D. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.
- E. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Answer: D

Explanation:

This answer is correct because AWS Shield Advanced is a service that provides comprehensive protection against DDoS attacks of any size or duration. It also provides metrics and reports on the DDoS attack vectors, duration, and size. You can create an Amazon CloudWatch alarm that monitors Shield Advanced metrics such as DDoSAttackBitsPerSecond, DDoSAttackPacketsPerSecond, and DDoSAttackRequestsPerSecond to receive alerts if a DDoS attack occurs against your account. For more information, see [Monitoring AWS Shield Advanced with Amazon CloudWatch and AWS Shield Advanced metrics and alarms](#).

NEW QUESTION 38

A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts. In addition, the company has an organization in IAM Organizations and has an IAM Security Hub master account. The security team wants to use Amazon Detective. However, the security team cannot enable Detective and is unsure why. What must the security team do to enable Detective?

- A. Enable Amazon Macie so that Security Hub will allow Detective to process findings from Macie.
- B. Disable IAM Key Management Service (IAM KMS) encryption on CloudTrail logs in every member account of the organization
- C. Enable Amazon GuardDuty on all member accounts. Try to enable Detective in 48 hours
- D. Ensure that the principal that launches Detective has the organizations:ListAccounts permission

Answer: D

NEW QUESTION 40

Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement. Please select:

- A. Set up VPC peering between the central server VPC and each of the teams VPCs.
- B. Set up IAM DirectConnect between the central server VPC and each of the teams VPCs.
- C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
- D. None of the above options will work.

Answer: A

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another IAM account within a single region. Options B and C are invalid because you need to use VPC Peering. Option D is invalid because VPC Peering is available. For more information on VPC Peering please see the below Link: <http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 44

A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of the web server.

The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance. Which combination of steps should the security engineer take to meet these requirements in the MOST secure manner? (Select TWO.)

- A. Allow port 22 from source 0.0.0.0/0.
- B. Allow port 443 from source 0.0.0.0/0.
- C. Allow port 22 from 192.168.100.0/24.
- D. Allow port 22 from 10.0.1.0/24.
- E. Allow port 443 from 10.0.1.0/24.

Answer: BC

Explanation:

The correct answer is B and C.

* B. Allow port 443 from source 0.0.0.0/0.

This is correct because port 443 is used for HTTPS traffic, which must be able to access the website from any source IP address.

* C. Allow port 22 from 192.168.100.0/24.

This is correct because port 22 is used for SSH, which is the management protocol for the web server. The management subnet is 192.168.100.0/24, so only this subnet should be allowed to access port 22.

* A. Allow port 22 from source 0.0.0.0/0.

This is incorrect because it would allow anyone to access port 22, which is a security risk. SSH should be restricted to the management subnet only.

* D. Allow port 22 from 10.0.1.0/24.

This is incorrect because it would allow the website subnet to access port 22, which is unnecessary and a security risk. SSH should be restricted to the management subnet only.

* E. Allow port 443 from 10.0.1.0/24.

This is incorrect because it would limit the HTTPS traffic to the website subnet only, which defeats the purpose of having a public website.

NEW QUESTION 48

A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.

The data includes personally identifiable information (PII). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table. Which solution will meet this requirement with the MOST operational efficiency?

- A. Update the Lambda function to add a TTL S3 flag to S3 object
- B. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
- C. Create an S3 Lifecycle policy to expire objects that are older than 30 day
- D. Update the Lambda function to add the TTL attribute in the DynamoDB tabl
- E. Enable TTL on the DynamoDB table to expire entires that are older than 30 days based on the TTL attribute.
- F. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucke
- G. Update the Lambda function to delete entries that are older than 30 days.
- H. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tag
- I. Update the Lambda function to delete entries that are older than 30 days.

Answer: B

NEW QUESTION 50

A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.

Which solution meets these requirements?

- A. Use IAM Systems Manager Parameter Store to store the database credential
- B. Configure automatic rotation of the credentials.
- C. Use IAM Secrets Manager to store the database credential
- D. Configure automat* rotation of the credentials
- E. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.
- F. Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the credentials on a scheduled bast

Answer: A

NEW QUESTION 52

An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": false
        }
      }
    }
  ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Change the value of aws:MultiFactorAuthPresent to true.
- B. Instruct users to run the `aws sts get-session-token` CLI command and pass the multi-factor authentication `--serial-number` and `--token-code` parameter
- C. Use these resulting values to make API/CLI calls.
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
- E. Create a role and enforce multi-factor authentication in the role trust policy
- F. Instruct users to run the `sts assume-role` CLI command and pass `--serial-number` and `--token-code` parameter
- G. Store the resulting values in environment variable
- H. Add `sts:AssumeRole` to `NotAction` in the policy.

Answer: B

Explanation:

The correct answer is B. Instruct users to run the `aws sts get-session-token` CLI command and pass the multi-factor authentication `--serial-number` and `--token-code` parameters. Use these resulting values to make API/CLI calls.

According to the AWS documentation¹, the `aws sts get-session-token` CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.

You can use the `--serial-number` and `--token-code` parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the `get-session-token` call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error. The temporary security credentials that are returned by the `get-session-token` command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.

Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.

The other options are incorrect because:

- > A. Changing the value of `aws:MultiFactorAuthPresent` to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA information to AWS for this condition key to be true.
- > C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the `get-session-token` command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.
- > D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the `get-session-token` command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the `sts assume-role` command instead of the `get-session-token` command.

References:

1: `get-session-token` — AWS CLI Command Reference

NEW QUESTION 55

A company is hosting a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The application has become the target of a DoS attack. Application logging shows that requests are coming from small number of client IP addresses, but the addresses change regularly.

The company needs to block the malicious traffic with a solution that requires the least amount of ongoing effort.

Which solution meets these requirements?

- A. Create an AWS WAF rate-based rule, and attach it to the ALB.
- B. Update the security group that is attached to the ALB to block the attacking IP addresses.
- C. Update the ALB subnet's network ACL to block the attacking client IP addresses.
- D. Create a AWS WAF rate-based rule, and attach it to the security group of the EC2 instances.

Answer: A

NEW QUESTION 57

A company uses a third-party identity provider and SAML-based SSO for its AWS accounts. After the third-party identity provider renewed an expired signing certificate, users saw the following message when trying to log in:

Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead. Which solution meets these requirements?

- A. Upload the third-party signing certificate's new private key to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS Management Console.
- B. Sign the identity provider's metadata file with the new public key
- C. Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.
- D. Download the updated SAML metadata file from the identity service provider
- E. Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.
- F. Configure the AWS identity provider entity defined in AWS Identity and Access Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

Answer: C

Explanation:

This answer is correct because downloading the updated SAML metadata file from the identity service provider ensures that AWS has the latest information about the identity provider, including the new public key. Updating the file in the AWS identity provider entity defined in IAM by using the AWS CLI allows AWS to verify the signature of the SAML assertions sent by the identity provider. This solution also minimizes operational overhead because it can be automated with a script or a cron job.

NEW QUESTION 59

A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The IAM account number is 111122223333, and the bucket name is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be implemented

Which statement should the security specialist include in the policy?

- A.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-server-side-encryption": "AES256"
    }
  }
}
```
- B.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
    }
  }
}
```
- C.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": "aws:kms"
    }
  }
}
```
- D.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLikeIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
    }
  }
}
```

- E. Option A
- F. Option B
- G. Option C
- H. Option D

Answer: D

NEW QUESTION 60

A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so

Which solution will meet these requirements?

- A. Create a new customer managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change
- B. Create a new AWS managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change
- C. Create a key alias Create a new customer managed key every time the security team requests a key change Associate the alias with the new key
- D. Create a key alias Create a new AWS managed key every time the security team requests a key change Associate the alias with the new key

Answer: A

Explanation:

To meet the requirement of changing the key material for new files whenever a potential key breach occurs, the most appropriate solution would be to create a new customer managed key, add a key rotation schedule to the key, and invoke the key rotation schedule every time the security team requests a key change.
 References: : Rotating AWS KMS keys - AWS Key Management Service

NEW QUESTION 65

A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired IAM accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use IAM managed services. What should the Security Engineer do to meet these requirements?

- A. Configure Amazon Macie to continuously check the configuration of all S3 buckets.
- B. Enable IAM Config to check the configuration of each S3 bucket.
- C. Set up IAM Systems Manager to monitor S3 bucket policies for public write access.
- D. Configure an Amazon EC2 instance to have an IAM role and a cron job that checks the status of all S3 buckets.

Answer: C

Explanation:

because this is a solution that can monitor each S3 bucket for unrestricted public write access and use IAM managed services. S3 is a service that provides object storage in the cloud. Systems Manager is a service that helps you automate and manage your AWS resources. You can use Systems Manager to monitor S3 bucket policies for public write access by using a State Manager association that runs a predefined document called AWS-FindS3BucketWithPublicWriteAccess. This document checks each S3 bucket in an account and reports any bucket that has public write access enabled. The other options are either not suitable or not feasible for meeting the requirements.

NEW QUESTION 69

A company is running workloads in a single IAM account on Amazon EC2 instances and Amazon EMR clusters a recent security audit revealed that multiple Amazon Elastic Block Store (Amazon EBS) volumes and snapshots are not encrypted The company's security engineer is working on a solution that will allow users to deploy EC2 Instances and EMR clusters while ensuring that all new EBS volumes and EBS snapshots are encrypted at rest. The solution must also minimize operational overhead Which steps should the security engineer take to meet these requirements?

- A. Create an Amazon Event Bridge (Amazon Cloud watch Events) event with an EC2 instance as the source and create volume as the event trigger
- B. When the event is triggered invoke an IAM Lambda function to evaluate and notify the security engineer if the EBS volume that was created is not encrypted.
- C. Use a customer managed IAM policy that will verify that the encryption ag of the Createvolume context is set to true
- D. Apply this rule to all users.
- E. Create an IAM Config rule to evaluate the configuration of each EC2 instance on creation or modification. Have the IAM Config rule trigger an IAM Lambda function to alert the security team and terminate the instance if the EBS volume is not encrypted
- F. 5
- G. Use the IAM Management Console or IAM CLI to enable encryption by default for EBS volumes in each IAM Region where the company operates.

Answer: D

Explanation:

To ensure that all new EBS volumes and EBS snapshots are encrypted at rest and minimize operational overhead, the security engineer should do the following:
 > Use the AWS Management Console or AWS CLI to enable encryption by default for EBS volumes in each AWS Region where the company operates. This allows the security engineer to automatically encrypt any new EBS volumes and snapshots created from those volumes, without requiring any additional actions from users.

NEW QUESTION 74

A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.

The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team. Which combination of solutions will meet these requirements? (Select TWO.)

- A. Create a local individual break glass IAM user for the security team
- B. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on
- C. Use Amazon EventBridge to monitor local user activities.
- D. Create a break glass EC2 key pair for the AWS account
- E. Provide the key pair to the security team
- F. Use AWS CloudTrail to monitor key pair activities
- G. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
- H. Create a break glass IAM role for the account
- I. Allow security team members to perform the AssumeRoleWithSAML operation
- J. Create an AWS Cloud Trail trail that has Amazon CloudWatch Logs turned on
- K. Use Amazon EventBridge to monitor security team activities.
- L. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
- M. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS Cloud Trail filter based on Session Manager
- N. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: AE

Explanation:

The combination of solutions that will meet the requirements are:

- A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge123.
- E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS456.

The other options are incorrect because:

- B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound ports on the instances and managing SSH keys, which increases the security risk and complexity7.
- C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors8.
- D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity9.

References:

1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

NEW QUESTION 79

A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.

Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

- A. Delete the access keys for the account root user in every account.
- B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
- C. Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.
- D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
- E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
- F. Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.

Answer: ADE

Explanation:

because these are the actions that can improve IAM account root user security. IAM account root user is a user that has complete access to all AWS resources and services in an account. IAM account root user security is a set of best practices that help protect the account root user from unauthorized or accidental use. Deleting the access keys for the account root user in every account can help prevent programmatic access by the account root user, which reduces the risk of compromise or misuse. Enabling MFA on every account root user in all accounts can help add an extra layer of security for console access by requiring a verification code in addition to a password. Creating a custom IAM policy to limit permissions to required actions for the account root user and attaching the policy to the account root user can help enforce the principle of least privilege and restrict the account root user from performing unnecessary or dangerous actions. The other options are either invalid or ineffective for improving IAM account root user security.

NEW QUESTION 83

A development team is attempting to encrypt and decode a secure string parameter from the IAM Systems Manager Parameter Store using an IAM Key Management Service (IAM KMS) CMK. However, each attempt results in an error message being sent to the development team.

Which CMK-related problems possibly account for the error? (Select two.)

- A. The CMK is used in the attempt does not exist.
- B. The CMK is used in the attempt needs to be rotated.
- C. The CMK is used in the attempt is using the CMK's key ID instead of the CMK ARN.
- D. The CMK is used in the attempt is not enabled.
- E. The CMK is used in the attempt is using an alias.

Answer: AD

Explanation:

<https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fa>

NEW QUESTION 84

A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS SSO to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- B. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.
- C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- D. For each AWS account, create tailored identity-based policies for AWS SS
- E. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

Answer: C

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-eleme

NEW QUESTION 86

A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time. Which solution will meet these requirements?

- A. Install the Amazon CloudWatch agent on each EC2 instance in the VP
- B. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log grou
- C. Use CloudWatch metric filters to automatically generate metrics that list the most common ONS queries.
- D. Install a BIND DNS server in the VP
- E. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.
- F. Create VPC flow logs for all subnets in the VP
- G. Stream the flow logs to an Amazon CloudWatch Logs log group
- H. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.
- I. Configure Amazon Route 53 Resolver query loggin
- J. Add an Amazon CloudWatch Logs log group as the destinatio
- K. Use Amazon CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/>

NEW QUESTION 89

A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated. What should the security engineer recommend?

- A. Enable Amazon RDS encryption to encrypt the database and snapshot
- B. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- C. Include the database credential in the EC2 user data fiel
- D. Use an AWS Lambda function to rotate database credential
- E. Set up TLS for the connection to the database.
- F. Install a database on an Amazon EC2 instanc
- G. Enable third-party disk encryption to encrypt Amazon Elastic Block Store (Amazon EBS) volum
- H. Store the database credentials in AWS CloudHSM with automatic rotatio
- I. Set up TLS for the connection to the database.
- J. Enable Amazon RDS encryption to encrypt the database and snapshot
- K. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- L. Store the database credentials in AWS Secrets Manager with automatic rotatio
- M. Set up TLS for the connection to the RDS hosted database.
- N. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS key
- O. Set up Amazon RDS encryption using AWS KSM to encrypt the databas
- P. Store the database credentials in AWS Systems Manager Parameter Store with automatic rotatio
- Q. Set up TLS for the connection to the RDS hosted database.

Answer: C

NEW QUESTION 92

A company uses AWS Organizations to manage several AWS accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate. The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key. What should the company do next to meet these requirements?

- A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoD
- B. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
- C. Create an IAM policy that denies the kms:Decrypt action for the ke
- D. Create a Lambda function than runs on a schedule to attach the policy to any new role
- E. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.
- F. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EK
- G. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
- H. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EK
- I. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Answer: B

NEW QUESTION 93

A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1 000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly. The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an IAM group for each application team
- B. Associate policies with each IAM group
- C. Provision IAM users for each application team member
- D. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).
- E. Delegate application team leads to provision IAM roles for each team
- F. Conduct a quarterly review of the IAM roles the team leads have provisioned
- G. Ensure that the application team leads have the appropriate training to review IAM roles.
- H. Put each AWS account in its own OU
- I. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use
- J. Include conditions in the AWS account of each team.
- K. Create an SCP and a permissions boundary for IAM roles
- L. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

Answer: D

Explanation:

To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required:

➤ Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization. An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization. SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see [Service control policies overview](#).

➤ Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see [Permissions boundaries for IAM entities](#).

➤ Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization.

This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified.

➤ Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access.

This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals.

The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible (C).

Verified References:

➤ https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 96

A company that uses AWS Organizations wants to see AWS Security Hub findings for many AWS accounts and AWS Regions. Some of the accounts are in the company's organization, and some accounts are in organizations that the company manages for customers. Although the company can see findings in the Security Hub administrator account for accounts in the company's organization, there are no findings from accounts in other organizations.

Which combination of steps should the company take to see findings from accounts that are outside the organization that includes the Security Hub administrator account? (Select TWO.)

- A. Use a designated administration account to automatically set up member accounts.
- B. Create the AWS Service Role For Security Hub service-linked role for Security Hub.
- C. Send an administration request from the member accounts.
- D. Enable Security Hub for all member accounts.
- E. Send invitations to accounts that are outside the company's organization from the Security Hub administrator account.

Answer: CE

Explanation:

To see Security Hub findings for accounts that are outside the organization that includes the Security Hub administrator account, the following steps are required:

➤ Send invitations to accounts that are outside the company's organization from the Security Hub administrator account. This will allow the administrator account to view and manage findings from those accounts. The administrator account can send invitations by using the Security Hub console, API, or CLI. For more information, see [Sending invitations to member accounts](#).

➤ Send an administration request from the member accounts. This will allow the member accounts to accept the invitation from the administrator account and establish a relationship with it. The member accounts can send administration requests by using the Security Hub console, API, or CLI. For more information, see [Sending administration requests](#).

This solution will enable the company to see Security Hub findings for many AWS accounts and AWS Regions, including accounts that are outside its own organization.

The other options are incorrect because they either do not establish a relationship between the administrator and member accounts (A, B), do not enable Security Hub for all member accounts (D), or do not use a valid service for Security Hub (E).

Verified References:

➤ <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-member-accounts.html>

NEW QUESTION 100

Your CTO is very worried about the security of your IAM account. How best can you prevent hackers from completely hijacking your account?

Please select:

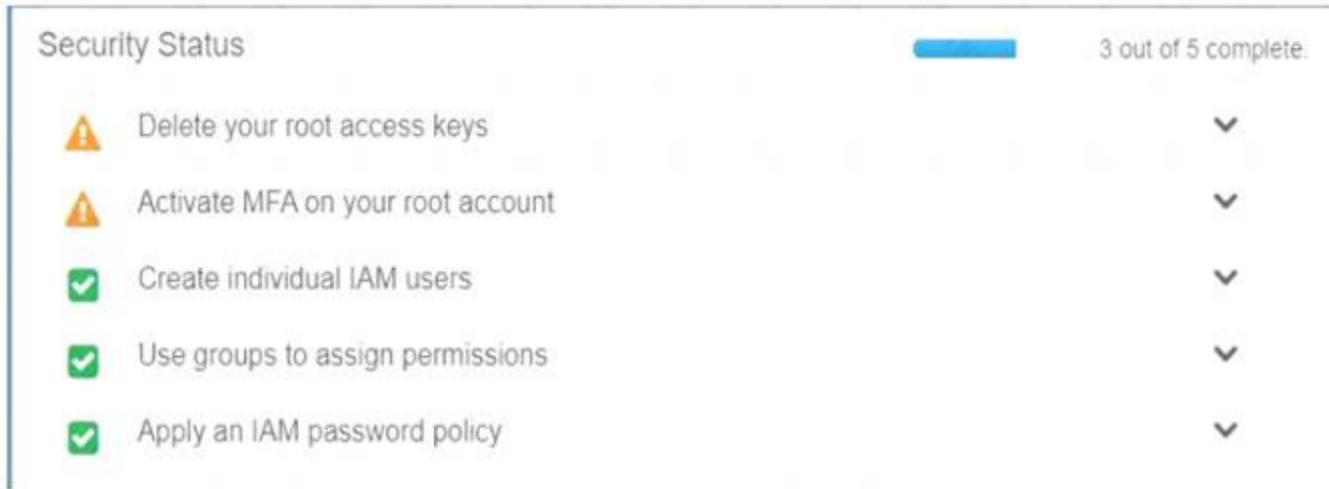
- A. Use short but complex password on the root account and any administrators.
- B. Use IAM Geo-Lock and disallow anyone from logging in except for in your city.
- C. Use MFA on all users and accounts, especially on the root account.
- D. Don't write down or remember the root account password after creating the IAM account.

Answer: C

Explanation:

Multi-factor authentication can add one more layer of security to your IAM account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because you need to have a good password policy Option B is invalid because there is no IAM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL

http://docs.IAM.amazonaws.com/IAM/latest/UserGuide/id_credentials_mfa.html

The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 103

A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.

Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.

The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.

Which solution will meet these requirements?

- A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
- B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.
- C. Enable CloudTrail Insights to identify unusual API activity.
- D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

Answer: D

Explanation:

The correct answer is D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets. According to the AWS documentation¹, CloudTrail data events are the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities. For example, Amazon S3 object-level API activity (such as GetObject, DeleteObject, and PutObject) is a data event.

By default, trails do not log data events. To record CloudTrail data events, you must explicitly add the supported resources or resource types for which you want to collect activity. For more information, see Logging data events in the Amazon S3 User Guide². In this case, the security team wants EventBridge to watch for the s3:PutObjectAcl API invocation logs from CloudTrail. This API uses the acl subresource to set the access control list (ACL) permissions for a new or existing object in an S3 bucket³. This is a data event that affects the S3 object resource type. Therefore, the security team must enable CloudTrail to monitor data events for read and write operations to S3 buckets in order to invoke an EventBridge event for this API call. The other options are incorrect because:

- > A. Modifying the EventBridge event pattern by selecting Amazon S3 and All Events as the event type will not capture the s3:PutObjectAcl API call, because this is a data event and not a management event. Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations⁴.
- > B. Modifying the EventBridge event pattern by selecting Amazon S3 and Bucket Level Operations as the event type will not capture the s3:PutObjectAcl API call, because this is a data event that affects the S3 object resource type and not the S3 bucket resource type. Bucket level operations are management events that affect the configuration or metadata of an S3 bucket⁵.
- > C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events⁶. It does not analyze data events or generate EventBridge events.

References:

1: CloudTrail log event reference - AWS CloudTrail 2: Logging data events - AWS CloudTrail 3: PutObjectAcl - Amazon Simple Storage Service 4: [Logging management events - AWS CloudTrail] 5: [Amazon S3 Event Types - Amazon Simple Storage Service] 6: Logging Insights events for trails - AWS CloudTrail

NEW QUESTION 105

A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off. What is the MOST efficient way to implement this solution?

- A. Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonaws.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.
- C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonaws.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.
- D. Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.

Answer: B

NEW QUESTION 107

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region. What policy should the Engineer implement?

A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

B. A computer code with black text Description automatically generated

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

C. A computer code with black text Description automatically generated

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

D. A computer code with text Description automatically generated

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

Answer: C

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.h

NEW QUESTION 108

A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration.

Which solution will meet this requirement?

- A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
- B. Specify the SES identity as the target for the EventBridge rule.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic
- D. Subscribe the third-party ticketing email system to the SNS topic
- E. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
- F. Specify the SNS topic as the target for the EventBridge rule.
- G. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
- H. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic
- I. Subscribe the third-party ticketing email system to the SNS topic.
- J. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
- K. Create an Amazon Simple Notification Service (Amazon SNS) topic
- L. Subscribe the third-party ticketing email system to the SNS topic
- M. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filter
- N. Specify the SNS topic as the target for the EventBridge rule.

Answer: B

Explanation:

The correct answer is B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.

According to the AWS documentation¹, you can use Amazon EventBridge to create rules that match events from GuardDuty and route them to targets such as Amazon SNS topics. You can use event patterns to filter events based on criteria such as severity, type, or resource. For example, you can create a rule that matches only High severity findings and sends them to an SNS topic that is subscribed by a third-party ticketing email system. This way, you can automate the creation of tickets for High severity findings and notify the security team.

NEW QUESTION 112

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.

A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.

Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

- A. Enable AWS Security Hub in the AWS account.
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for GuardDuty findings of high severity
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for Security Hub findings of high severity
- J. Configure the rule to publish a message to the queue.

Answer: BCE

NEW QUESTION 116

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile. However, three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties. How can a security engineer provide the access to meet these requirements'?

- A. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager. Provide the 1AM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Inventory to select the EC2 instance and connect.
- B. Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command. Remove the SSH keys from the EC2 instances. Use Run Command to open an SSH connection to the EC2 instance.
- C. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager. Provide the 1AM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Session Manager to select the EC2 instance and connect.
- D. Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console. Remove the SSH keys from the EC2 instances. Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method.

Answer: C

Explanation:

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect.

References: : AWS Systems Manager Session Manager - AWS Systems Manager : AWS Systems Manager AWS Management Console : AWS Identity and Access Management - AWS Management Console : Amazon Elastic Compute Cloud - Amazon Web Services : Amazon Linux 2 - Amazon Web Services : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console

NEW QUESTION 117

A company deployed Amazon GuardDuty in the us-east-1 Region. The company wants all DNS logs that relate to the company's Amazon EC2 instances to be inspected. What should a security engineer do to ensure that the EC2 instances are logged?

- A. Use IPv6 addresses that are configured for hostnames.
- B. Configure external DNS resolvers as internal resolvers that are visible only to IAM.
- C. Use IAM DNS resolvers for all EC2 instances.
- D. Configure a third-party DNS resolver with logging for all EC2 instances.

Answer: C

Explanation:

To ensure that the EC2 instances are logged, the security engineer should do the following:

- Use AWS DNS resolvers for all EC2 instances. This allows the security engineer to use Amazon-provided DNS servers that resolve public DNS hostnames to private IP addresses within their VPC, and that log DNS queries in Amazon CloudWatch Logs.

NEW QUESTION 122

A company is planning to use Amazon Elastic File System (Amazon EFS) with its on-premises servers. The company has an existing IAM Direct Connect connection established between its on-premises data center and an IAM Region. Security policy states that the company's on-premises firewall should only have specific IP addresses added to the allow list and not a CIDR range. The company also wants to restrict access so that only certain data center-based servers have access to Amazon EFS.

How should a security engineer implement this solution?

- A. Add the file-system-id efs IAM-region amazonIAM.com URL to the allow list for the data center firewall. Install the IAM CLI on the data center-based servers to mount the EFS file system in the EFS security group. Add the data center IP range to the allow list. Mount the EFS using the EFS file system name.
- B. Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall. Install the IAM CLI on the data center-based servers to mount the EFS file system. In the EFS security group, add the IP addresses of the data center servers to the allow list. Mount the EFS using the Elastic IP address.
- C. Add the EFS file system mount target IP addresses to the allow list for the data center firewall. In the EFS security group, add the data center server IP addresses to the allow list. Use the Linux terminal to mount the EFS file system using the IP address of one of the mount targets.
- D. Assign a static range of IP addresses for the EFS file system by contacting IAM Support. In the EFS security group, add the data center server IP addresses to the allow list. Use the Linux terminal to mount the EFS file system using one of the static IP addresses.

Answer: B

Explanation:

To implement the solution, the security engineer should do the following:

- Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall. This allows the security engineer to use a specific IP address for the EFS file system that can be added to the firewall rules, instead of a CIDR range or a URL.
- Install the AWS CLI on the data center-based servers to mount the EFS file system. This allows the security engineer to use the mount helper provided by AWS CLI to mount the EFS file system with encryption in transit.
- In the EFS security group, add the IP addresses of the data center servers to the allow list. This allows the security engineer to restrict access to the EFS file system to only certain data center-based servers.
- Mount the EFS using the Elastic IP address. This allows the security engineer to use the Elastic IP address as the DNS name for mounting the EFS file system.

NEW QUESTION 127

A company uses an external identity provider to allow federation into different IAM accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.

What is the FASTEST way for the security engineer to identify the federated user?

- A. Review the IAM CloudTrail event history logs in an Amazon S3 bucket and look for the TerminateInstances event to identify the federated user from the role session name.
- B. Filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role.
- C. Review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username.
- D. Search the IAM CloudTrail logs for the TerminateInstances event and note the event time.
- E. Review the IAM Access Advisor tab for all federated roles.
- F. The last accessed time should match the time when the instance was terminated.
- G. Use Amazon Athena to run a SQL query on the IAM CloudTrail logs stored in an Amazon S3 bucket and filter on the TerminateInstances event.
- H. Identify the corresponding role and run another query to filter the AssumeRoleWithWebIdentity event for the user name.

Answer: B

Explanation:

The fastest way to identify the federated user who terminated a production Amazon EC2 instance is to filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role. Then, review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username. This method does not require any additional tools or queries, and it directly links the IAM role with the federated user.

Option A is incorrect because the role session name may not be the same as the federated user name, and it may not be unique or descriptive enough to identify the user.

Option C is incorrect because the IAM Access Advisor tab only shows when a role was last accessed, not by whom or for what purpose. It also does not show the specific time of access, only the date.

Option D is incorrect because using Amazon Athena to run SQL queries on the IAM CloudTrail logs is not the fastest way to identify the federated user, as it requires creating a table schema and running multiple queries. It also assumes that the federation is done using web identity providers, not SAML providers, as indicated by the AssumeRoleWithWebIdentity event.

References:

- > AWS Identity and Access Management
- > Logging AWS STS API Calls with AWS CloudTrail
- > [Using Amazon Athena to Query S3 Data for CloudTrail Analysis]

NEW QUESTION 131

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS Cloud Trail trail in the same Region to deliver log files to an Amazon S3 bucket by using the AWS CLI.

Because of expansion, the company adds resources in multiple Regions. The security engineer notices that the logs from the new Regions are not reaching the S3 bucket.

What should the security engineer do to fix this issue with the LEAST amount of operational overhead?

- A. Create a new CloudTrail trail
- B. Select the new Regions where the company added resources.
- C. Change the S3 bucket to receive notifications to track all actions from all Regions.
- D. Create a new CloudTrail trail that applies to all Regions.
- E. Change the existing CloudTrail trail so that it applies to all Regions.

Answer: D

Explanation:

The correct answer is D. Change the existing CloudTrail trail so that it applies to all Regions.

According to the AWS documentation¹, you can configure CloudTrail to deliver log files from multiple Regions to a single S3 bucket for a single account. To change an existing single-Region trail to log in all Regions, you must use the AWS CLI and add the `--is-multi-region-trail` option to the `update-trail` command². This will ensure that you log global service events and capture all management event activity in your account.

Option A is incorrect because creating a new CloudTrail trail for each Region will incur additional costs and increase operational overhead. Option B is incorrect because changing the S3 bucket to receive notifications will not affect the delivery of log files from other Regions. Option C is incorrect because creating a new CloudTrail trail that applies to all Regions will result in duplicate log files for the original Region and also incur additional costs.

NEW QUESTION 134

A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way?

`{resolve:s3:MyBucketName:MyObjectName}}`.

- A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store
- B. In the template, replace all references to the value with `{{resolve:ssm:MySSMParameterName:}}`.
- C. Store the API key value in AWS Secrets Manager
- D. In the template, replace all references to the value with `{{resolve:secretsmanager:MySecretId:SecretString}}`.
- E. Store the API key value in Amazon DynamoDB
- F. In the template, replace all references to the value with `{{resolve:dynamodb:MyTableName:MyPrimaryKey}}`.
- G. Store the API key value in a new Amazon S3 bucket
- H. In the template, replace all references to the value with `{`

Answer: B

Explanation:

The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with `{{resolve:secretsmanager:MySecretId:SecretString}}`.

This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle¹. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the

`{{resolve:secretsmanager:...}}` syntax². This way, you can avoid exposing your secrets in plaintext and still use them in your resources.

The other options are incorrect because:

- A. Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters. This means that you cannot use the `{{resolve:ssm:...}}` syntax to retrieve encrypted parameter values from Parameter Store³. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.
- C. Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the `{{resolve:dynamodb:...}}` syntax to retrieve item values from DynamoDB tables⁴. You would have to use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.
- D. Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the `{{resolve:s3:...}}` syntax to retrieve object values from S3 buckets⁵. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.

References:

1: What is AWS Secrets Manager? 2: Referencing AWS Secrets Manager secrets from Parameter Store parameters 3: Using dynamic references to specify template values 4: Amazon DynamoDB 5: Amazon Simple Storage Service (S3)

NEW QUESTION 137

A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days. Which solution meets these criteria?

- A. A customer managed CMK that uses customer provided key material
- B. A customer managed CMK that uses AWS provided key material
- C. An AWS managed CMK
- D. Operation system-native encryption that uses GnuPG

Answer: A

Explanation:

```
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/kms/import-key-material.html aws kms import-key-material \
--key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
--encrypted-key-material fileb://EncryptedKeyMaterial.bin \
--import-token fileb://ImportToken.bin \
--expiration-model KEY_MATERIAL_EXPIRES \
--valid-to 2021-09-21T19:00:00Z
```

The correct answer is A. A customer managed CMK that uses customer provided key material.

A customer managed CMK is a KMS key that you create, own, and manage in your AWS account. You have full control over the key configuration, permissions, rotation, and deletion. You can use a customer managed CMK to encrypt and decrypt data in AWS services that are integrated with AWS KMS, such as Amazon EBS¹.

A customer managed CMK can use either AWS provided key material or customer provided key material. AWS provided key material is generated by AWS KMS and never leaves the service unencrypted. Customer provided key material is generated outside of AWS KMS and imported into a customer managed CMK. You can specify an expiration date for the imported key material, after which the CMK becomes unusable until you reimport new key material².

To meet the criteria of automatically expiring the key material in 90 days, you need to use customer provided key material and set the expiration date accordingly. This way, you can ensure that the data encrypted with the CMK will not be accessible after 90 days unless you reimport new key material and re-encrypt the data. The other options are incorrect for the following reasons:

- * B. A customer managed CMK that uses AWS provided key material does not expire automatically. You can enable automatic rotation of the key material every year, but this does not prevent access to the data encrypted with the previous key material. You would need to manually delete the CMK and its backing key material to make the data inaccessible³.
- * C. An AWS managed CMK is a KMS key that is created, owned, and managed by an AWS service on your behalf. You have limited control over the key configuration, permissions, rotation, and deletion. You cannot use an AWS managed CMK to encrypt data in other AWS services or applications. You also cannot set an expiration date for the key material of an AWS managed CMK⁴.
- * D. Operation system-native encryption that uses GnuPG is not a solution that uses AWS KMS. GnuPG is a command line tool that implements the OpenPGP standard for encrypting and signing data. It does not integrate with Amazon EBS or other AWS services. It also does not provide a way to automatically expire the key material used for encryption⁵.

References:

1: Customer Managed Keys - AWS Key Management Service 2: [Importing Key Material in AWS Key Management Service (AWS KMS) - AWS Key Management Service] 3: [Rotating Customer Master Keys - AWS Key Management Service] 4: [AWS Managed Keys - AWS Key Management Service] 5: The GNU Privacy Guard

NEW QUESTION 141

A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events to an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No logs are being received.

What should the Security Engineer do to troubleshoot this issue?

- A) Add the following statement to the IAM managed CMKs:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

B)
 Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sns.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

C)
 Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sqs.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

D)
 Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 146

A security engineer has enabled IAM Security Hub in their IAM account, and has enabled the Center for internet Security (CIS) IAM Foundations compliance standard. No evaluation results on compliance are returned in the Security Hub console after several hours. The engineer wants to ensure that Security Hub can evaluate their resources for CIS IAM Foundations compliance.

Which steps should the security engineer take to meet these requirements?

- A. Add full Amazon Inspector IAM permissions to the Security Hub service role to allow it to perform the CIS compliance evaluation
- B. Ensure that IAM Trusted Advisor Is enabled in the account and that the Security Hub service role has permissions to retrieve the Trusted Advisor security-related recommended actions
- C. Ensure that IAM Confi
- D. is enabled in the account, and that the required IAM Config rules have been created for the CIS compliance evaluation
- E. Ensure that the correct trail in IAM CloudTrail has been configured for monitoring by Security Hub and that the Security Hub service role has permissions to perform the GetObject operation on CloudTrails Amazon S3 bucket

Answer: C

Explanation:

To ensure that Security Hub can evaluate their resources for CIS AWS Foundations compliance, the security engineer should do the following:

- Ensure that AWS Config is enabled in the account. This is a service that enables continuous assessment and audit of your AWS resources for compliance.
- Ensure that the required AWS Config rules have been created for the CIS compliance evaluation. These are rules that represent your desired configuration settings for specific AWS resources or for an entire AWS account.

NEW QUESTION 151

A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native IAM features should be used as much as possible. The security engineer has set up IAM Organizations with all features activated and IAM SSO enabled.

Which additional steps should the security engineer take to complete the task?

- A. Use AD Connector to create users and groups for all employees that require access to IAM accounts. Assign AD Connector groups to IAM accounts and link to the IAM roles in accordance with the employees' job functions and access requirements. Instruct employees to access IAM accounts by using the IAM Directory Service user portal.
- B. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account.
- C. Assign groups to IAM accounts and link to permission sets in accordance with the employees' job functions and access requirement.
- D. Instruct employees to access IAM accounts by using the IAM SSO user portal.
- E. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account.
- F. Link IAM SSO groups to the IAM users present in all accounts to inherit existing permission.
- G. Instruct employees to access IAM accounts by using the IAM SSO user portal.
- H. Use IAM Directory Service for Microsoft Active Directory to create users and groups for all employees that require access to IAM accounts. Enable IAM Management Console access in the created directory and specify IAM SSO as a source of information for integrated accounts and permission set.
- I. Instruct employees to access IAM accounts by using the IAM Directory Service user portal.

Answer: B

NEW QUESTION 154

A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses.

The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.

Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connections. Use the IP addresses from these remote connections to create deny rules in the security group of the instance. Install diagnostic tools on the instance for investigation. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- B. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule. Replace the security group with a new security group that allows connections only from a diagnostics security group. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule. Launch a new EC2 instance that has diagnostic tools. Assign the new security group to the new EC2 instance. Use the new EC2 instance to investigate the suspicious instance.
- C. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination. Terminate the instance. Launch a new EC2 instance in us-east-1a that has diagnostic tools. Mount the EBS volumes from the terminated instance for investigation.
- D. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance. Attach the AWS WAF web ACL to the instance to mitigate the attack. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: B

Explanation:

This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.

NEW QUESTION 157

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

- A. Amazon Route 53
- B. IAM Certificate Manager (ACM)
- C. Amazon S3
- D. IAM Shield
- E. Elastic Load Balancer
- F. Amazon GuardDuty

Answer: DEF

NEW QUESTION 161

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.

How can a security engineer meet this requirement?

- A. Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).
- B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect forward secrecy (PFS).
- C. Create an HTTPS listener that uses the Server Order Preference security feature.

D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Answer: A

NEW QUESTION 164

A team is using AWS Secrets Manager to store an application database password. Only a limited number of IAM principals within the account can have access to the secret. The principals who require access to the secret change frequently. A security engineer must create a solution that maximizes flexibility and scalability. Which solution will meet these requirements?

- A. Use a role-based approach by creating an IAM role with an inline permissions policy that allows access to the secret
- B. Update the IAM principals in the role trust policy as required.
- C. Deploy a VPC endpoint for Secrets Manager
- D. Create and attach an endpoint policy that specifies the IAM principals that are allowed to access the secret
- E. Update the list of IAM principals as required.
- F. Use a tag-based approach by attaching a resource policy to the secret
- G. Apply tags to the secret and the IAM principal
- H. Use the `aws:PrincipalTag` and `aws:ResourceTag` IAM condition keys to control access.
- I. Use a deny-by-default approach by using IAM policies to deny access to the secret explicitly
- J. Attach the policies to an IAM group
- K. Add all IAM principals to the IAM group
- L. Remove principals from the group when they need access
- M. Add the principals to the group again when access is no longer allowed.

Answer: C

NEW QUESTION 166

A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.

Which combination of steps must the company perform to meet this requirement? (Select TWO.)

- A. Create an identity policy that allows the `sts: AssumeRole` action in the AWS account that contains the resource
- B. Attach the identity policy to the IAM user.
- C. Ensure that the `sts: AssumeRole` action is allowed by the SCPs of the organization that owns the resources that the IAM user needs to access.
- D. Create a role in the AWS account that contains the resource
- E. Create an entry in the role's trust policy that allows the IAM user to assume the role
- F. Attach the trust policy to the role.
- G. Establish a trust relationship between the IAM user and the AWS account that contains the resources.
- H. Create a role in the IAM user's AWS account
- I. Create an identity policy that allows the `sts: AssumeRole` action
- J. Attach the identity policy to the role.

Answer: BC

Explanation:

To allow cross-account access to resources using IAM roles, the following steps are required:

- Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
- Ensure that the IAM user has permission to assume the role in their own AWS account. This can be done by creating an identity policy that allows the `sts: AssumeRole` action and attaching it to the IAM user or their group.
- Ensure that there are no service control policies (SCPs) in the organization that owns the resources that deny or restrict access to the `sts: AssumeRole` action or the role itself. SCPs are applied to all accounts in an organization and can override any permissions granted by IAM policies.

Verified References:

- <https://repost.aws/knowledge-center/cross-account-access-iam>
- https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
- https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION 169

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

AWS-Certified-Security-Specialty Practice Exam Features:

- * AWS-Certified-Security-Specialty Questions and Answers Updated Frequently
- * AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff
- * AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The AWS-Certified-Security-Specialty Practice Test Here](#)